

Federal Communications Commission EDU2011 Wireless Pilot Program Proposal

Submitted December 17, 2010

Applicant General Information:

Dover Area School District
2 School Lane
Dover, PA 17315

District E-rate Entity Number: 125758

Public School District located in York County, Pennsylvania

Contact Person: Dana Baker, Assistant Superintendent

Email: dbaker@dover.k12.pa.us

Phone: 717-292-3671

Fax: 717-292-9659

Required Information (All Applicants):

1. Full Description of current program:

- A. The Dover Area School District formed an online school in June, 2009 after a full year of planning. The online school is named the Dover Cyber Academy and designed to serve students in grades K-12. The school has been in operation for two school years (2009/10 and 2010/11). The curriculum associated with students taking online courses involving hardware and Internet access are paid by the Dover Area SD general fund budget.

The curriculum is based upon the PA Academic Standards. The students that are enrolled in the Dover Cyber Academy participate in all local assessments provided by the district as well as the Pennsylvania System of School Assessment. During the first two years of operation, data has been collected regarding performance of the students and compared to the traditional classroom students. No significant difference (positive or negative) has been identified in student achievement. Students from all district schools may participate in the online academy including:

Dover High School, entity number 18418
Dover Intermediate School, Entity number 18419
North Salem Elementary School, entity number 204522
Dover Elementary School, entity number 18420
Weiglestown Elementary School, entity number 18423
Kralltown Elementary School, entity number 18425
Leib Elementary School, entity number 18422

- B. The Dover Areas School District has operated the cyber school for two years including summer months of credit recovery as well as enrichment courses. The wireless laptops have been in use since the start of the online school.
- C. When the school researched the feasibility of starting an online learning venue, several items became clear obstacles very early in the planning process:

Approximately 20% of the students did not have functional computers in their homes. Of the 80% of the homes that did have computers, 10% had no Internet connectivity due to economic considerations. And another 10% of the homes with computers did not have Internet speeds necessary to support the online instructional content.

The district had to revise the "Acceptable Use Policy" to include off campus users of district provided technology.

As a result the planning team for the school district online school decided to provide the hardware and wireless access necessary to participate in online courses for all student participants.

- D. All staff actively involved in Dover Cyber Academy have been trained in content development software "Blackboard" at various levels of need:
 - a. Online course development
 - b. Online course revision and updates
 - c. Online instructional strategies
 - d. Administration of online schools
 - E. The Dover Cyber Academy has agreed to provide online course content for adult job training and high school diploma programs. Cyber school staff have met with the York County Development Authority to provide cost effective job re-training programs online.
2. The Dover Area School District poverty level is 34.7 % (district average) and the overall E-rate discount level is 50%.
 3. The school district has no industry within the district tax base area and is predominantly a suburban/rural community with predominantly service-based employers. In the past 2 years there has been a major increase in unemployment which is in the 10%-12% range. The average per capita income is now at \$26,100. The school district is large at over 60 square miles. The district's ability to raise revenues is now severely impacted by the inability of residents to pay additional property taxes. It is now necessary for the district to choose the option of reducing staff to balance budgets.
 4. The total district costs per full-time online elementary student are \$2950 per year for 5 online courses. The district cost per secondary students (Grade 7-12) for 6 online courses is \$3650. These totals include software, prorated hardware, wireless access, teacher support, and all miscellaneous costs.
 5. The district has allocated funding to provide online courses to 100 students for the current budget year as well as the 2011/12 budget year. Currently the cyber school has 51 students enrolled as full or part-time students and 22 staff members serve the school.

6. If the E-rate discount is applied to the wireless Internet access cards, the school district will save \$21,120 per year as the access fee is currently \$44 per month per card (\$44 * 80 laptops * 12 months * 50% E-rate discount). The resulting savings will be used to offset other budgetary obligations in the district and enhance the cyber school offerings. The School District Cyber School currently has 80 net books with wireless cards in operation for delivery of online courses.
7. The district's delivery of online instruction without the use of wireless technology would have required "hard wire" systems to each home including in many cases, installation costs by vendors. The cost comparison compared wireless to "hard wire" systems indicated an additional fee of over \$50 for the first month (service establishment fee). The wireless cost did not require a service establishment fee. The largest saving was the actual cost of net book due to the vendor contract providing the net book at approximately \$200 per unit compared to \$600 average cost per unit. (This vendor agreement provided a pre-installed wireless card in a net book similar to establishing an account with a cell phone provider and obtaining a lower cost for the hardware.)
8. The Dover School District Technology Plan approved by the board that includes the establishment of an online school is attached.
9. See attached district policy for compliance information, "Children's Internet Protection Act."
10. See attached district policy for compliance information, "Acceptable Use of Wireless Internet."

Attachments

1. Dover Area SD Internet Acceptable Use Policy
2. Dover Area SD Technology Plan submitted to the Pennsylvania Department of Education

<p>1. Purpose</p>	<p style="text-align: center;">815. ACCEPTABLE USE OF COMPUTER TECHNOLOGY</p> <p>The purpose of this policy is to outline the acceptable uses of technology, including, but not limited to, hardware devices, software, and Internet access in the Dover Area School District and to define the consequences of misuse. For the purpose of this document, a user is defined as administrator, teacher, student, community member, invited guest, or other individuals employed by Dover Area School District.</p> <p>Dover Area School District networks and computing resources exist to support the instructional and administrative needs of the district. Networks and computing resources are critical information sources. It is our goal to provide technological services that promote educational excellence in</p>
-------------------	---

	<p>schools by facilitating resource sharing, innovation, and communication.</p> <p>Smooth operation of the district's computer networks and access to the Internet relies upon the proper conduct of the end users that must adhere to strict guidelines. These guidelines are provided here so that you are aware of the responsibilities that you are about to acquire. In general, this requires efficient, ethical and legal utilization of the network information resources. If a user violates any of these provisions, his/her account will be disabled. Future access to computer technology could possibly be denied.</p>
2. Definitions	<p>The Dover Area School District technology includes any school district-owned, leased or licensed or user-owned personal hardware, software, or other technology used on school district premises or at school district events, or connected to the school district network, containing school district programs or school district or student data (including images, files, and other information) attached or connected to, installed in, or otherwise used in connection with a computer. Computer includes, but is not limited to, school district and users': desktop, notebook, tablet PC or laptop computers, printers, facsimile machine, cables, modems, and other peripherals; specialized electronic equipment used for students' special educational purposes; global positioning system (GPS) equipment; personal digital assistants (PDAs); iPods, MP3 players; cell phones, with or without Internet access and/or recording and/or camera/video and other capabilities; mobile phones or wireless devices; two-way radios/telephones; beepers, and other paging devices, local area networking and wide area networking devices, as well as all online networking such as the Internet to which the school network may be linked.</p>
3. Authority	<p>The electronic information available to users does not imply endorsement of the content by the school district, nor does the district guarantee the accuracy of information received on the Internet. The district shall not be responsible for any information that may be lost, damaged or unavailable when using the network, or for any information that is retrieved via the Internet.</p> <p>The school district shall not be responsible for any charges or fees resulting from unauthorized access to the Internet.</p> <p>It is often necessary to access user accounts in order to perform routine maintenance and security tasks; system administrators have the right to access, by interception, the stored information of users for any reason in order to uphold this policy and to maintain the system. Users have no privacy expectation in the contents of their personal files or any of their use of the school district's network. The school district reserves the right to monitor, track, log and access school district's network use and to monitor and allocate fileserver space.</p>

<p>4. Guidelines</p>	<p>The Board establishes use of the district networks and other computing resources as a privilege, not a right. Inappropriate, unauthorized and illegal use of these networks and/or computer resources may result in the cancellation of those privileges and appropriate disciplinary action. District network administrators have the right to deny, revoke, or suspend specific use.</p> <p>The school district has the right, but not the duty, to monitor, track, log, access and/or report all aspects of its computer information, technology and related systems of all users and of any user's personal computers, network, Internet, electronic communication systems, and media that s/he brings onto school district property, or to school district events, that were connected to the school district network, which contained school district programs or school district or student data (including but not limited to images, and files), in order to ensure compliance with this policy and other school district policies, to protect the school district's resources, and to comply with the law.</p> <p>All users of Dover Area School District technology must sign a Technology Acceptable Use Agreement prior to using the computers.</p> <p>Students may only access the Internet after reading their Student Handbook, Use of Dover Area School District Computer Network/Internet, and the student's parent/guardian has indicated their preference on the Emergency Card. This permission is granted for one (1) year and must be renewed every year to gain access to Internet resources.</p> <p><u>Security</u></p> <p>System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or district files. To protect the integrity of the system, the following guidelines shall be followed:</p> <ol style="list-style-type: none"> 1. Any user provided a password shall not reveal his/her password to another individual.
----------------------	---

<p>SC 1303.1-A</p> <p>Pol. 249</p>	<ol style="list-style-type: none"> 2. Users are not to use a computer that has been logged in under another student's or employee's name. 3. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network. <p><u>Prohibitions</u></p> <p>Users are expected to act in a responsible, ethical and legal manner in accordance with district policy, accepted rules of network etiquette, and federal and state law. Specifically the following uses are prohibited:</p> <ol style="list-style-type: none"> 1. Network accounts are to be used only by the authorized owner of the account for the authorized purpose. 2. Any violation of the use of the district computing resources should be reported to the appropriate administrator. 3. No use of the network shall serve to disrupt the use of the network by others. Hardware or software shall not be abused, modified, or destroyed. 4. Malicious use of the network to harass other users or infiltrate a computer or computing system is prohibited. 5. Hate mail, harassment, discriminatory remarks, bullying/cyber bullying and other antisocial behaviors are prohibited on the network. 6. Use of the network to access or print pornographic materials, inappropriate text files, or files dangerous to the integrity of the local or wide area networks is prohibited. 7. Users may not alter in any way a network or computing resource, device, peripheral, file, or folder names. 8. Users may not copy applications, folders, or files unless it is directly related to curriculum projects and it follows all other established policies and guidelines.
------------------------------------	--

<p>17 U.S.C. Sec. 101 et seq Pol. 814</p>	<ol style="list-style-type: none"> 9. Users may not distribute or alter network or computing resource passwords. 10. Users may not use any network or computing resource for personal entertainment or private activities. 11. Users may not use any network or computing resource to gain unauthorized access to other networks or computing resources. 12. Users may not violate any software or other licensing agreements. 13. Users are expected to adhere to Section 117 of the 1976 Copyright Act as amended in 1980. 14. Individual computing classrooms or areas may impose printing restrictions on any or all users in that area. 15. Vandalism will result in cancellation of user privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another user of the network or the Internet, or the software and hardware belonging to the Dover Area School District. This includes, but is not limited to, the uploading or creating of computer viruses. 16. Users may not bypass or attempt to bypass Internet filtering software by any method including, but not limited to, the use of anonymizers/proxies or any web sites that mask the content the user is accessing or attempting to access. <p><u>Software</u></p> <p>All software used by the district on district-owned computers will be purchased through the technology department. All software is to be delivered to the technology department for completion of registration and inventory requirements. Software must be registered in the name of the Dover Area School District.</p> <p>All software will be authorized and installed by the technology department. The technology department may approve other users to install a specific software program on a specific computer(s). Once software is installed, the original media will be kept in a storage area maintained by the technology department.</p>
---	--

Netiquette

While using the Dover Area School District network, users are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

1. Be polite. Use appropriate language. Do not swear, use vulgarities, or any other inappropriate or offensive language.
2. Do not reveal your personal address or phone number, or those of any other person.
3. Electronic mail (e-mail) is not guaranteed to be private. District network administrators have the right to monitor electronic mail messages. Messages relating to or in support of illegal activities shall be reported to the authorities.
4. It is the user's responsibility to maintain the integrity of the private electronic mail system. The user has the responsibility to report all unauthorized violations of privacy. Users have the responsibility to make only those contacts leading to some justifiable professional or academic growth on the Internet. The user is also responsible for making sure all e-mail sent or received does not contain pornographic material, inappropriate information, or text-encoded files that are potentially dangerous to the integrity of the local area network or the Internet.
5. Do not use the network in such a way that would disrupt the use of the network by other users.

INTERNET SAFETY

General Warning: Individual Responsibility Of Parents/Guardians And Users

All users and their parents/guardians are advised that access to the electronic network may include the potential for access to materials inappropriate for school-aged pupils. Every user must take

responsibility for his/her use of the computer network and Internet and stay away from these sites. If a user finds that other users are visiting offensive or harmful sites, s/he should report such use to his/her supervising teacher.

Personal Safety

Be safe. In using the computer network and Internet, do not reveal personal information such as your home address or telephone number. Do not use your real last name or any other information which might allow a person to locate you without first obtaining the permission of a supervising teacher. Do not arrange a face-to-face meeting with someone you meet on the computer network or Internet. If someone attempts to arrange a meeting with you as a result of an Internet contact, you must report the communication immediately to your supervising teacher.

Hacking And Other Illegal Activities

It is a violation of this policy to use the district's computer network or the Internet to gain unauthorized access to other computers or computer systems, or to attempt to gain such unauthorized access. Any use which violates state or federal law relating to copyright, trade secrets, the distribution of obscene or pornographic materials, or any other applicable law or municipal ordinance is strictly prohibited.

Confidentiality Of Student Information

Personally identifiable information concerning students may not be disclosed or used in any way on the Internet without the permission of a parent/guardian or the student if over eighteen (18) years

	<p>of age. Users should never give out private or confidential information about themselves or others on the Internet, particularly credit card numbers and Social Security numbers. Only a member of the school administration may authorize the release of student information.</p> <p><u>Active Restriction Measures</u></p>
<p>20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254</p>	<p>The district, either by itself or in combination with an Internet Service Provider (ISP), will utilize filtering software or other technologies to prevent users from accessing visual depictions that are: (1) obscene, (2) child pornography, or (3) harmful to minors. The district will also monitor the online activities of users, through direct observation and/or technological means, to ensure that users are not accessing such depictions or any other material that is inappropriate for minors.</p> <p>Internet filtering software or other technology-based protection systems may be disabled by the Technology Coordinator or his/her designee, as necessary, for purposes of valid research or other educational projects being conducted by a user(s).</p>
<p>20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254</p>	<p>The term harmful to minors is defined as meaning any picture, image, graphic image file, or other visual or written depiction that:</p> <ol style="list-style-type: none"> 1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion. 2. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals. 3. Lacks serious literary, artistic, political, or scientific value as to minors.

Privacy

The district reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage. All such information files shall be and remain the property of the district and no user shall have any expectation of privacy regarding such materials.

Violation Of Policy

Use of the computer network and Internet is a privilege, not a right. A user who violates this policy, shall, at a minimum, have his/her access to the computer network and Internet terminated, which the district may refuse to reinstate for the remainder of the student's enrollment in the district. A user violates this policy by his/her own action or by failing to report any violations by other users that come to the attention of the user. Further, a user violates this policy if s/he permits another to use his/her account or password to access the computer network and Internet, including any user whose access has been denied or terminated. The district may also take other disciplinary action in such circumstances. In some instances, inappropriate computer and Internet use violates state and/or federal laws and may result in criminal prosecution or juvenile court action.

Warranties/Indemnification

The district makes no warranties of any kind, either express or implied, in connection with its provision of access to and use of its computer networks and the Internet provided under this policy. The district shall not be responsible for any claims, losses, damages or costs (including fees) of any kind suffered, directly or indirectly, by any user or his/her parent(s)/guardian(s) arising out of the use of its computer networks or the Internet under this policy. By signing this policy, the user is taking full responsibility for his/her use, and the user who is eighteen (18) or older

or, in the case of a user under eighteen (18), the parent(s)/guardian(s), are agreeing to indemnify and hold the district, administrators, professional employees, and staff harmless from any and all loss, costs, claims or damages resulting from the user's access to its computer network and the Internet, including but not limited to any fees or charges incurred through purchases of goods or services by the user. The user or, if the user is a minor, the user's parent(s)/guardian(s), agree to

<p>Pol. 218, 317, 417, 517</p>	<p>cooperate with the district in the event of the district's initiating an investigation of a user's access to the computer network and the Internet.</p> <p><u>Updates</u></p> <p>Users, or the user's parents/guardians, may be asked to provide new or additional registration and account information or to sign a new policy. The policy must be signed if the user wishes to continue to receive service. If after you have provided your account information, some or all of the information changes, you must notify the building principal.</p> <p><u>Consequences</u></p> <p>The violations on the preceding pages are not all inclusive, but only representative and illustrative. A user who commits an act of misconduct which is not listed may also be subject to disciplinary action.</p> <p>Disciplinary actions are based on the discipline procedures of the Dover Area School District.</p> <p>Administrators may use any or all of the following suggested intervention strategies and disciplinary action.</p> <p><i>Minimum Actions –</i></p> <ol style="list-style-type: none"> 1. Administrator/Teacher/Student conference. 2. Administrator/Teacher/Student verbal and/or written reprimand. <p><i>Additional Actions As Deemed Appropriate –</i></p> <ol style="list-style-type: none"> 1. Administrator/Parental contact. 2. Referrals and conferences involving various support staff or agencies.
------------------------------------	--

	<ol style="list-style-type: none"> 3. Behavioral contracts. 4. Required serving of a minimum of one-day suspension from using all district computer equipment. 5. Confiscation of inappropriate items. 6. Restitution/Restoration, including any professional services required. 7. Denial of participation in class activities. 8. Banned from access to the Internet for a specified number of days. 9. Banned from using all computer equipment, networks, or Internet. 10. In-school suspension. 11. Out-of-school suspension. 12. Expulsion. 13. Other intervention strategies as needed. 14. Subject to criminal prosecution under state and federal laws. <p><u>Copyright</u></p> <p>The illegal use of copyrighted software by students and staff is prohibited. Any data uploaded to or downloaded from the network shall be subject to fair use guidelines.</p>
Pol. 814	
5. Delegation of	The district shall make every effort to ensure that this educational resource is used responsibly by

Responsibility	<p>students, staff, and community members.</p> <p>The building administrator and/or the district Technology Coordinator shall have the authority to determine what is inappropriate use. His/Her decision is final.</p> <p>The viewing of movies for recreational activities is not educational fair use. A specific license is required for recreational activities within Dover Area School District buildings and may be obtained by contacting the Technology Coordinator. The completion of a license form and payment of a fee are required.</p> <p>References:</p> <p>School Code – 24 P.S. Sec. 1303.1-A</p> <p>State Board of Education Regulations – 22 PA Code Sec. 403.1</p> <p>Child Internet Protection Act – 24 P.S. Sec. 4601 et seq.</p> <p>U.S. Copyright Law – 17 U.S.C. Sec. 101 et seq.</p> <p>Enhancing Education Through Technology Act of 2001 – 20 U.S.C. Sec. 6777</p>
----------------	--

	<p>Internet Safety – 47 U.S.C. Sec. 254</p> <p>Board Policy – 218, 249, 317, 417, 517, 814</p>
--	--